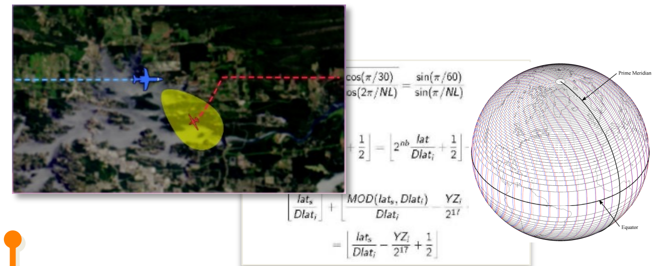
Natasha A. Neogi, Sarah M. Lehman
NASA Langley Research Center (LaRC)

PROBLEMS IN MACHINE LEARNING-BASED SYSTEMS FOR SAFETY-CRITICAL AVIONICS

DARPA PROPOSERS' DAY - THURS. FEB. 17, 2022

Safety-Critical Avionics Systems Branch

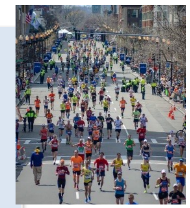


Application and advancement of formal methods for specifying and verifying correctness and safety properties

Safety assessment and assurance methods

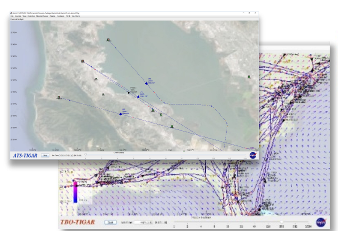
- SC-186: Automatic Dependent Su… Broadcast
- SC-205: Software Considerations… Aeronautical Systems
- CAST –Airplane State Awareness… Analysis Team (JSAT)
- SC-228: Minimum Operational Pe… Standards for Unmanned Aircraft
- SC-203: Unmanned Aircraft Syste…
- …

- Streamlining Assurance via Overarching Properties
- Automated Rapid Certification of Software
- Examination of Time-Triggered Ethernet in the Integrated Artemis Architecture
- 4D prognostics to forecast GPS quality in urban environments
- Backup systems for Global…



	Frequent	Probable	Occasional	Remote
Catastrophic	Action required to eliminate or control hazard	Action required to eliminate or control hazard	Action required to eliminate or control hazard	Control hazard or reduce probability
Hazardous	Action required to eliminate or control hazard	Action required to eliminate or control hazard	Control hazard or reduce probability	Hazard control desirable
Major	Action required to eliminate or control hazard	Control hazard or reduce probability	Hazard control desirable	Hazard control not required

Architectural and runtime V&V for assuring system-level integrity

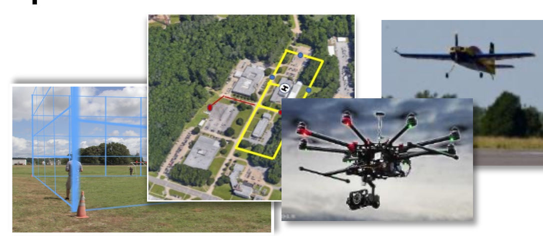


ICAROUS

DAIDALUS

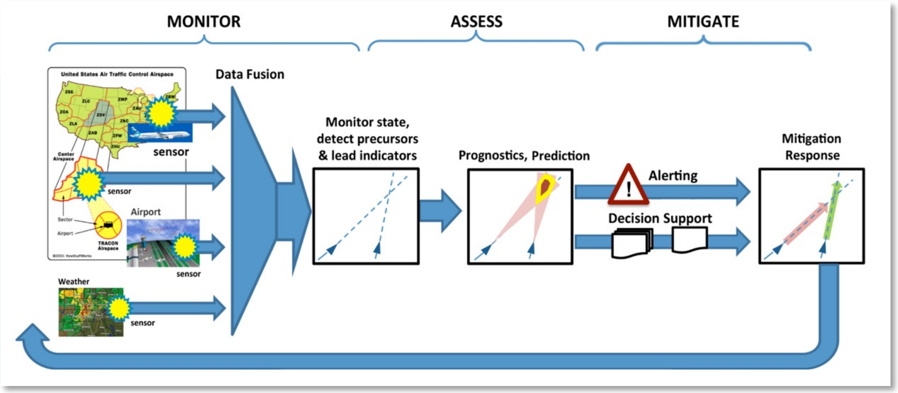
Highly-assured algorithms for aerospace applications

Integrated experimental testing for evaluating blended design and operational assurance constructs



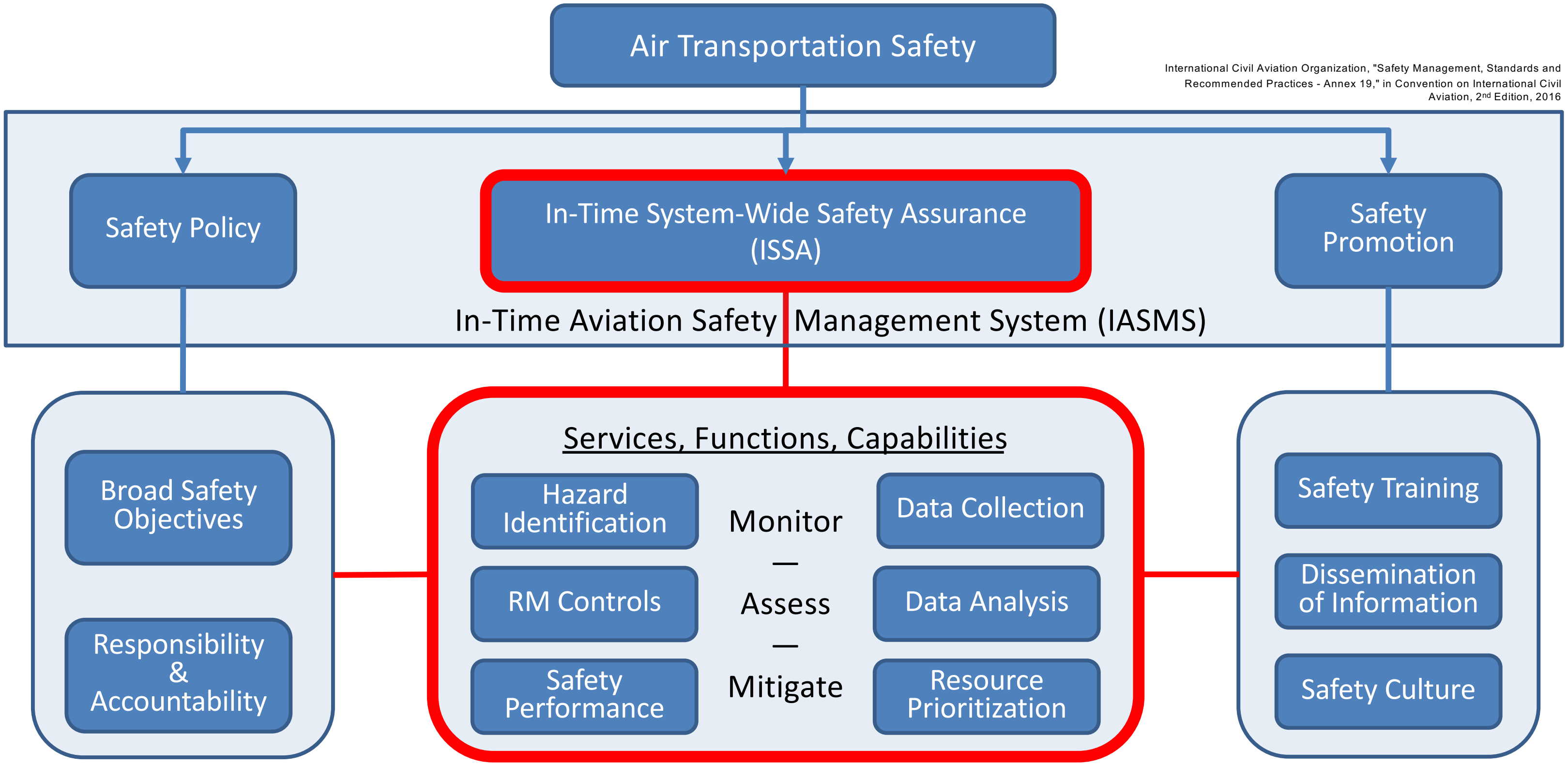
System-Wide Safety Project Objectives

To explore, discover, and understand
the impact on safety of growing complexity introduced by modernization aimed at improving the efficiency of flight, the access to airspace, and/or the expansion of services provided by air vehicles.



To develop and demonstrate
innovative solutions that enable this modernization and the aviation transformation envisioned by ARMD through proactive mitigation of risks in accordance with target levels of safety.

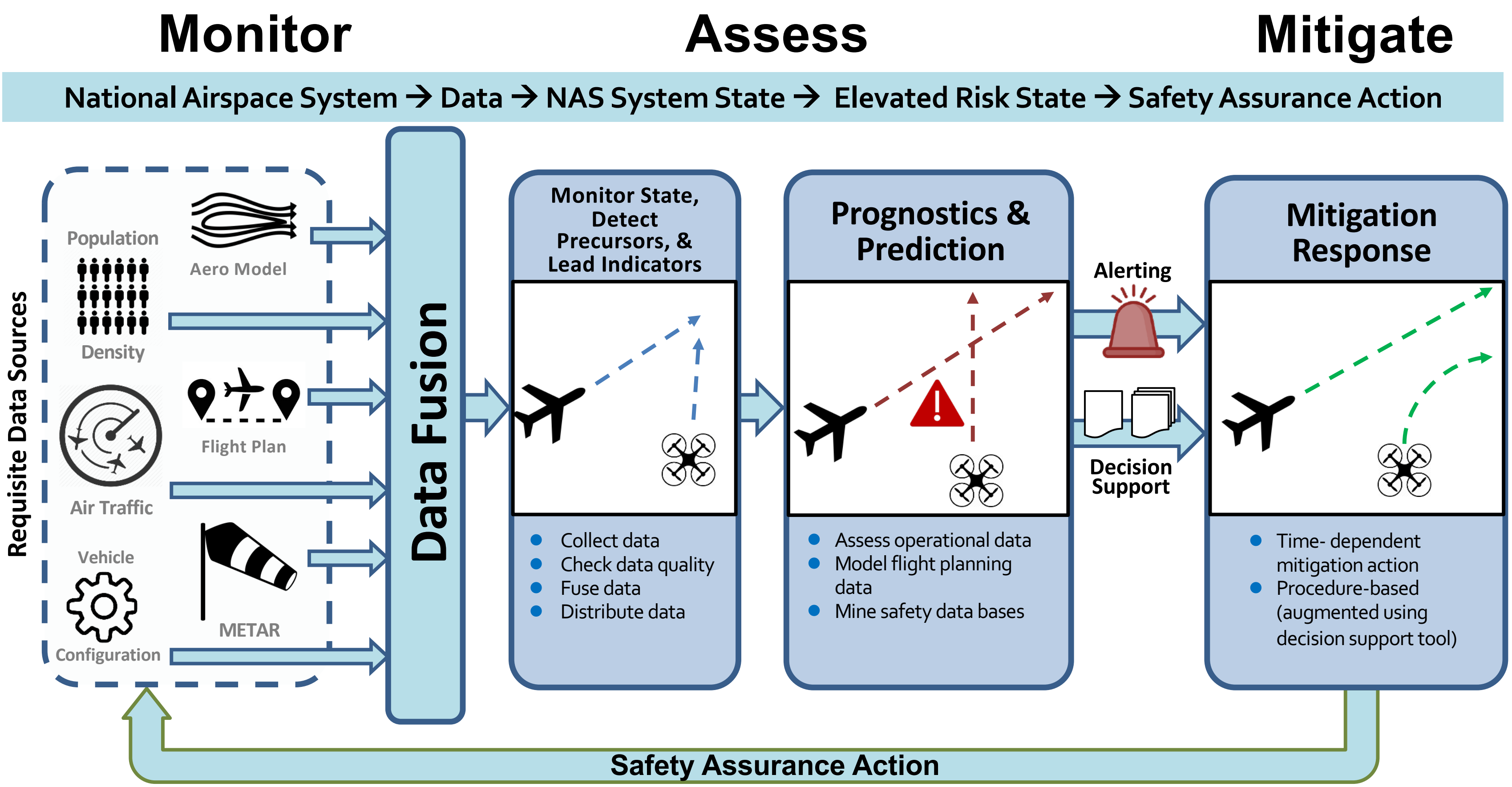
How We Achieve Aviation Safety Tomorrow



International Civil Aviation Organization, "Safety Management, Standards and Recommended Practices - Annex 19," in Convention on International Civil Aviation, 2nd Edition, 2016

Services, Functions, and Capabilities Execute Risk Management and Safety Assurance Actions

Services, Functions, and Capabilities (SFCs)



SWS Overview – Safety Demonstrator Series

Operational Safety (Thrust 5)

TC-1: ***Predictive Terminal Area Risk Assessment***

TC-2: ***IASMS SFC Development for Emerging Operations***

Current Day

Near Future

TC-3: ***V&V for Commercial Operations***

TC-4: ***Complex Autonomous Systems Assurance***

Design Safety (Thrust 6)

Through a series of operationally challenging demonstrations, develop and demonstrate a system-wide safety framework that enables increasingly complex airspace operations.

TC-5: Safety Demonstrator Series for Operational IASMS

SD-1: Wildfire Fighting (FY25)
SD-2: Post-Hurricane Disaster Relief
SD-3: Medical Courier Delivery (Urban Environment)
SD-4: Un-evacuated Urban Area Disaster Response

Problem #1 – N-fold Testing of ML Models

Scenario: developing new machine learning modules for safety-critical applications
- Must meet some "certainty threshold" for satisfying safety properties
- Must be able to handle edge cases arising from real-world use

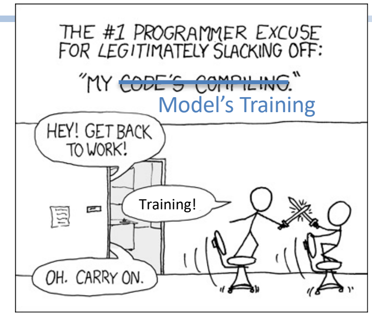


IMAGE SOURCE: https://xkcd.com/303/

Problem: How to develop new time- and resource-efficient testing practices for machine learning models that assure safety properties during real-world use
- True understanding of how ML components make decisions is limited
- Testing approaches for traditional software systems do not extend to ML systems
- Training, validating, testing ML components requires both time and processing power

Potential FastNICs Contributions:
- **Speed up model training, testing** – improve throughput of cross-validation activities, performance comparisons across multiple data sets which requires many model re-trainings
- **Enable parallelized data collection** – gathering, analyzing contextual data in real-time (environmental conditions, device resource consumption traces, etc.) can assist in debugging misclassifications from the system-under-test
- **Enable ML component redundancy, confederation** – leveraging results from additional models run in real-time can also help highlight errors from the system-under-test

Anticipated Impact:
- Would allow us to develop more comprehensive test suites for new ML components without having to dedicate massive amounts of time and compute resources to their execution

(a) Classifier error generates wrong warning text

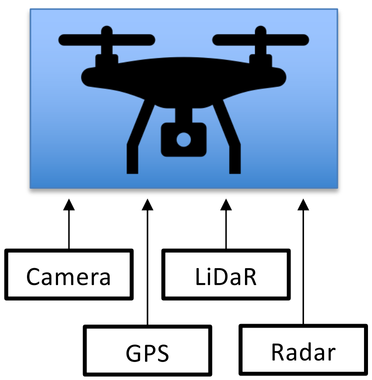
(b) Slow processing, quick user movement prevents classification

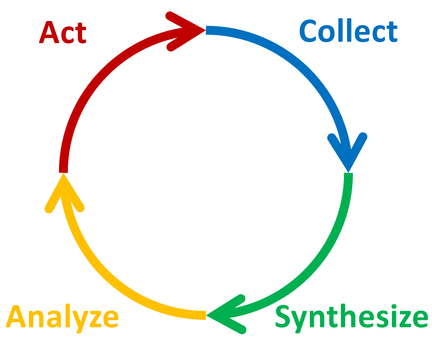
(c) Poor label placement covers pertinent real-world content (car in intersection)

(d) Alert correctly placed but difficult to read due to poor color choice

IMAGE SOURCE: Lehman, Sarah M., Haibin Ling, and Chiu C. Tan. "ARCHIE: A user-focused framework for testing augmented reality applications in the wild." *2020 IEEE Conference on Virtual Reality and 3D User Interfaces (VR).* IEEE, 2020.

Problem #2 – Multi-sensor Feeds for UAS Detect-and-Avoid





Scenario: UAS flying autonomously with local detect-and-avoid capabilities

- Equipped with multiple onboard sensors and processors
- Continuously executing data collection, processing activities
- ML components trained offline, updated between missions

Problem: How to improve accuracy, reliability of real-time data aggregation and processing capabilities on resource-constrained devices such as UAS's

- Managing multiple data feeds, performing ML operations in real time
- Maintaining trade-off between accuracy and resource consumption

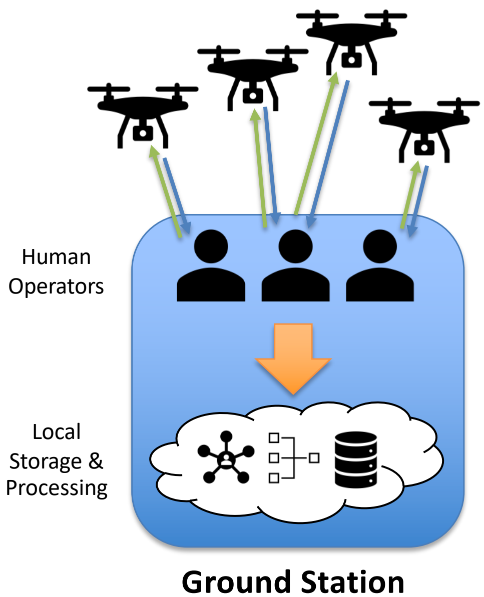
Potential FastNICs Contributions:

- **Enable ML component redundancy** – perform an ML operation with an independent secondary version of the module to verify preliminary results
- **Enable ML component confederation** – perform operations and vote on a result among a group of independent candidate modules

Anticipated Impact:

- Improve reliability of autonomous decision-making capabilities of UASs in the field; provide backups to primary ML components to mitigate runtime errors

Problem #3 – Surveillance, Assessment, and Analysis



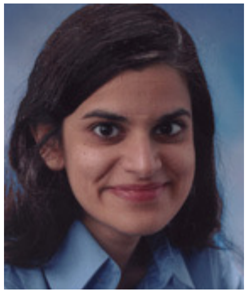
Scenario: (m) operators managing (N) UAS's to monitor a wildfire situation
- Operators control multiple vehicles each (N >> m) from ground station
- Vehicles provide streaming service only; no on-board processing
- Data aggregated, processed at ground station

Problem: How to improve streaming bandwidth, processing latency in ad hoc networks of station-controlled UAS's
- Balancing network traffic with resource cost for UAS's
- Minimizing processing latency at ground station for real-time situational awareness

Potential FastNICs Contributions:
- **Support low-energy, high-bandwidth wireless transmissions** – allow the UAS to offload data, receive commands without using too much power
- **Support high-bandwidth ML operations** – allow the ground station to perform an open-ended number of ML operations on the collected data and make informed decisions in real-time

Anticipated Impact:
- Improve data collection, processing, and assessment capabilities to improve situational awareness, and to identify and respond to issues as they arise

Thank you! Questions?



Natasha A. Neogi
natasha.a.neogi@nasa.gov

Sarah M. Lehman
sarah.lehman@nasa.gov